FIGURE 1 is a block diagram illustrating communication between facilities during the registration phase according to an aspect of the present invention;

FIGURE 1A is a flow chart of the communication between facilities of FIGURE 1 during the registration phase according to an aspect of the present invention;

FIGURE 2 is a block diagram illustrating interaction between facilities during the pre-voting phase according to an aspect of the present invention;

FIGURE 2A is a flow chart of the interaction between facilities of FIGURE 2 during the pre-voting phase according to an aspect of the present invention;

FIGURE 3 is a block diagram illustrating interaction between facilities during the voting phase according to an aspect of the present invention;

FIGURE 3A is a flow chart of the interaction between facilities of FIGURE 3 during the voting phase according to an aspect of the present invention;

FIGURE 4 is a sample ballot and a sample matching pair according to an aspect of the present invention;

FIGURE 4A is a flow chart of the interaction between facilities of FIGURE 1 during the announcement phase according to an aspect of the present invention;

FIGURE 5 is a block diagram illustrating an election system according to an aspect of the present invention;

FIGURE 6 is a block diagram illustrating some details of a registrar of FIGURE 5 according to an aspect of the present invention;

FIGURE 7 is a block diagram illustrating some details of an authenticator of FIGURE 5 according to an aspect of the present invention;

FIGURE 8 is a block diagram illustrating some details of a verifier of FIGURE 5 according to an aspect of the present invention;

FIGURE 9 is a block diagram illustrating some details of a tally system of FIGURE 5 according to an aspect of the present invention;

FIGURE 10 is a block diagram illustrating some details of a matcher of FIGURE 9 according to an aspect of the present invention;

FIGURE 11 is a block diagram illustrating some details of a counter of FIGURE 9 according to an aspect of the present invention; and

FIGURE 12 is a block diagram illustrating some details of a distributor of FIGURE 9 according to an aspect of the present invention.--.

Please add the following new paragraphs on page 29 of the Substitute Specification immediately after line 23: --

Referring now to the drawings in general and Figure 5 in particular, it will be understood that the illustrations are for the purpose of describing preferred embodiments of the invention and are not intended to limit the invention thereto. As best seen in Figure 5, an election system, generally designated 10, is shown constructed according to an embodiment of the present invention. In this embodiment, the election system 10 includes a registrar 12, a plurality of ballots 14 as depicted in Figure 3, a plurality of authentication codes 112, a data reconciler 18, and a tally system 34. As seen in Figures 5 and 6, the registrar 12 includes a registrar link 20 that permits communication with at least a plurality of voters 22. For example, the registrar link 20 permits a voter 28 of the plurality of voters 22 to obtain a unique voter ID 24 by registering with the registrar 12. The plurality of ballots 14 is for distribution to at least a portion of the plurality of voters 22. Each ballot includes a unique ballot ID 26 and a corresponding list of plain data 30 (sometimes herein referred to as a plain text version). The plurality of authentication codes 112 is generated such that one authentication code 112 is used with a corresponding cast ballot of the plurality of ballots 14. As seen in Figure 5, the data reconciler 18 includes a data reconciler link 32 for communication to at least the registrar 12. Also, as seen in Figures 5 and 9, the tally system 34 includes a tally system link 36 for communication to at least the data reconciler 18.

In an alternative embodiment according to the present invention, an election system 10 includes a registrar 12, a plurality of ballots 14 and a data reconciler 18. The registrar 12 includes a registrar link 20 that permits communication. For example, the registrar link 20 permits a voter 28 of the plurality of voters 22 to obtain a unique voter ID 24 by registering with the registrar 12. At least a portion of the plurality of ballots 14 is for distribution to at least a portion of the plurality of voters 22. Each ballot includes a unique ballot ID 26 and a corresponding list of plain data 30. The data reconciler 18 includes a data reconciler link 32 for communication to at least the registrar 12.

In still another alternative embodiment of the present invention, an election system 10 includes a registrar 12, a plurality of ballots 14, a plurality of authentication codes 112 and a data reconciler 18. The registrar 12 includes a registrar link 20 that permits communication. For example, the registrar link 20 permits a voter 28 of the plurality of voters 22 to obtain a unique voter ID 24 by registering with the registrar 12. At least a portion of the plurality of ballots 14 is for distribution to at least a portion of the plurality of voters 22. Each ballot may include a unique ballot ID 26 and a corresponding list of plain data 30. The plurality of authentication codes 112 is generated such that one authentication code 112 is used with a corresponding cast ballot of the plurality of ballots 14. The data reconciler 18 includes a data reconciler link 32 for communication to at least the registrar 12.

As seen in Figures 5, 9 and 11, the election system 10 includes a counter 40. As depicted in Figure 11, the counter 40 of election system 10 includes a counter link 42, a ballot generator 44, a ballot authenticator 64, a counter database 72, a counter key generator 74, a counter database encryptor 76, and a counter database decryptor 80. The counter link 42 of the counter 40 provides for communication within at least the election system 10.

The ballot generator 44 generates the plurality of ballots 14. A secure ballot generator is preferred. As depicted in Figure 11, the ballot generator 44 includes a

matching pair generator 46, a ballot encryption key generator 52, a ballot encryptor 56, and a ballot decryption key generator 60. The matching pair generator 46 generates a matching pair 50 corresponding to each unique ballot ID 26 and each corresponding list of plain data 30 for each ballot of the plurality of ballots 14. The ballot encryption key generator 52 generates a plurality of ballot encryption keys 54 corresponding to each of the plurality of ballots 14. A preferred ballot encryption key generator 52 is a ballot encryption key-decryption key pair generator. The ballot encryptor 56 encrypts the corresponding list of plain data 30 for each of the plurality of ballots 14 using the corresponding plurality of ballot encryption keys 54. The ballot decryption key generator 60 generates a plurality of ballot decryption keys 62 corresponding to the plurality of ballots 14 to facilitate decryption thereof. As noted, the ballot encryption key generator 52 may be a ballot encryption key-decryption key pair generator in which case the ballot decryption key generator 60 may be part of the ballot encryption key generator 52

The ballot authenticator 64 authenticates cast ballots. As depicted in Figure 11, the ballot authenticator 64 includes a tallier 66 and a decryptor 70. The tallier 66 tallies cast ballots, preferably after the cast ballots have been determined to be authentic. The decryptor 70 decrypts cast ballots prior to tallying cast ballots.

The counter database 72 includes at least the unique ballot IDs 26 of the plurality of ballots 14. As depicted in Figure 11, counter database 72 further includes a ballot decryption key 62, the plurality of ballots 14, matching pairs 50, and ballot encryption key 54. Each ballot decryption key 62, matching pair 50 and ballot encryption key 54 set corresponds to a unique ballot ID 26 of the plurality of ballots 14.

As depicted in Figure 11, the counter key generator 74 is a public key-private key pair generator. The counter database encryptor 76 encrypts data prior to storing the data in the counter database 72. A preferred counter database encryptor 76 is an on the fly

encryptor. The counter database encryptor 76 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the counter database 72.

As depicted in Figure 11, decryption of data within the counter database 72 by the counter database decryptor 80 may be necessary prior to one having the ability to access the data. A preferred counter database decryptor 80 is a partial decryptor.

As seen in Figures 5, 9 and 10, the election system 10 includes a matcher 82. As depicted in Figure 10, the matcher 82 of election system 10 includes a matcher link 84, a matcher database 86, a matcher key generator 90, a matcher database encryptor 92, and a matcher database decryptor 94. The matcher link 84 is for communication at least within the election system 10 and in particular with the plurality of voters 22.

The matcher database 86 has at least a matching pair 50 corresponding to each of the unique ballot IDs 26 of the plurality of ballots 14.

As depicted in Figure 10, the matcher key generator 90 is a public key-private key pair generator. The matcher database encryptor 92 encrypts data prior to storing the data in the matcher database 86. A preferred matcher database encryptor 92 is an on the fly encryptor. The matcher database encryptor 92 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the matcher database 86.

As depicted in Figure 10, decryption of data within the matcher database 86 by the matcher database decryptor 94 may be necessary prior to one having the ability to access the data. A preferred matcher database decryptor 94 is a partial decryptor.

As seen in Figures 5, 9 and 12, the election system 10 includes a distributor 96. As depicted in Figure 10, the distributor 96 of election system 10 includes a distributor link 100, a distributor database 102, a distributor key generator 104, a distributor database encryptor 106, and a distributor database decryptor 110. The distributor link 100 is for

communication at least within the election system 10 and in particular with the plurality of voters 22. The distributor database 102 has at least the plurality of ballots 14.

As depicted in Figure 12, the distributor key generator 104 is a public key-private key pair generator. The distributor database encryptor 106 encrypts data prior to storing the data in the distributor database 102. A preferred distributor database encryptor 106 is an on the fly encryptor. The distributor database encryptor 106 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the distributor database 102.

As depicted in Figure 12, decryption of data within the distributor database 102 by the distributor database decryptor 110 may be necessary prior to one having the ability to access the data. A preferred distributor database decryptor 110 is a partial decryptor.

As depicted in Figure 4, the plurality of ballots 14 includes the list of plain data 30 and an encrypted version 114 thereof.

The data reconciler 18 provides the authentication code 112. One alternative for the authentication code 112 is an encrypted version 114 of the list of plain data 30. The encrypted version 114 of the list of plain data 30 is provided to the distributor 96 for proving to the plurality of voters 22.

As depicted in Figure 4, the plurality of matching pairs 50 corresponds to an encrypted version 114 of the list of plain data 30. The data reconciler 18 provides the plurality of matching pairs 50. In particular, the plurality of matching pairs 50 is provided to the matcher 82 for distribution to the plurality of voters 22.

As seen in Figures 5 and 6, the election system 10 includes the registrar 12. As depicted in Figure 6, the registrar 12 of election system 10 includes a registrar link 20, a voter identifier 116, a registrar database 120, a registrar key generator 124, a registrar database encryptor 126, a voter ID generator 134, and a registrar database decryptor 130. The registrar link 20 is for communication at least within the election system 10 and in

particular with the plurality of voters 22. A preferred registrar link 20 is bi-directional. To that end, the registrar link 20 may be an Internet link 132.

The voter identifier 116 is determining the identity of the plurality of voters 22 that have cast a vote. As depicted in Figure 6, the registrar database 120 includes voter information 122 such as voter names 128 and unique voter ID 24 of the plurality of voters 22.

As depicted in Figure 6, the registrar key generator 124 is a public key-private key pair generator. The registrar database encryptor 126 encrypts data prior to storing the data in the registrar database 120. A preferred registrar database encryptor 126 is an on the fly encryptor. The registrar database encryptor 126 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the registrar database 120.

As depicted in Figure 6, decryption of data within the registrar database 120 by the registrar database decryptor 130 may be necessary prior to one having the ability to access the data. A preferred registrar database decryptor 130 is a partial decryptor.

The unique voter ID 24 facilitates communication between a voter 28 of the plurality of voters 22 and the data reconciler 18. Also, the unique voter ID 24 facilitates communication between a voter 28 of the plurality of voters 22 and the registrar 12. Moreover, the unique voter ID 24 permits a voter 28 of the plurality of voters 22 to obtain a ballot of the plurality of ballots 14. Also, the unique voter ID 24 permits verifying that a voter 28 of the plurality of voters 22 has cast a ballot of the plurality of ballots 14.

As depicted in Figure 6, the unique voter ID generator 134 includes a counter 136 for determining the number of unique IDs generated. The registrar link 20 facilitates providing the unique voter ID 24 from the data reconciler 18 to a voter 28. Moreover, the registrar link 20 facilitates providing a voter private key 140 to a voter 28 of the plurality of voters 22. In a preferred embodiment, the registrar 12 passes the voter private key 140

to the voter 28 of the plurality of voters 22 without keeping a copy of the voter private key 140.

As seen in Figures 5 and 7, the election system 10 includes an authenticator 142. As depicted in Figure 7, the authenticator 142 of election system 10 includes an authenticator link 144, a voter authenticator 146, an authenticator database 150, a voter key generator 154, a voter authenticator key generator 156, an authenticator database encryptor 160, and an authenticator database decryptor 162. The authenticator link 144 is for communication at least within the election system 10 and in particular with at least the registrar 12. The authenticator database 150 includes a plurality of voter ID-decryption key pairs 152. Preferred voter ID-decryption key pairs 152 are voter ID-voter public key pairs.

The voter key generator 154 is a voter decryption key generator. A preferred voter key generator 154 is a voter public key-private key pair generator.

As depicted in Figure 7, the authenticator key generator 156 is a public key-private key pair generator. The authenticator database encryptor 160 encrypts data prior to storing the data in the authenticator database 150. A preferred authenticator database encryptor 160 is an on the fly encryptor. The authenticator database encryptor 160 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the authenticator database 150.

As depicted in Figure 7, decryption of data within the authenticator database 150 by the authenticator database decryptor 162 may be necessary prior to one having the ability to access the data. A preferred authenticator database decryptor 162 is a partial decryptor.

As seen in Figures 5 and 8, the election system 10 includes a verifier 164. As depicted in Figure 8, the verifier 164 of election system 10 includes a verifier link 166, a vote counter 170, a verifier database 174, a verifier key generator 176, a verifier database encryptor 180, and a verifier database decryptor 182. The authenticator link 166 is for communication at least within the election system 10. The vote counter 170 counts cast

ballots to verify a vote tally. A preferred vote counter 170 facilitates the independent counting of cast ballots to verify a vote tally. The vote counter 170 includes a ballot decryptor 172 for decrypting cast ballots to permit the vote counting of the vote tally.

The verifier database 174 includes a plurality of ballot ID-decryption key pairs 168. Preferred ballot ID-decryption key pairs 168 are ballot ID-voter public key pairs.

As depicted in Figure 8, the verifier key generator 176 is a public key-private key pair generator. The verifier database encryptor 180 encrypts data prior to storing the data in the verifier database 174. A preferred verifier database encryptor 180 is an on the fly encryptor. The verifier database encryptor 180 preferably uses public keys generated by a plurality of facilities of the election system 10 to encrypt the verifier database 174.

As depicted in Figure 8, decryption of data within the verifier database 174 by the a verifier database decryptor 182 may be necessary prior to one having the ability to access the data. A preferred a verifier database decryptor 182 is a partial decryptor.

A data reconciler link 32 permits communication with a voter 28 of the plurality of voters 22. A preferred communication method with a voter 28 is via an Internet link 132. Alternatively, a communication with a voter 28 is via an Intranet link. Communication with a voter 28 may be direct; it may be indirect.--.